Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 19, брой 2, 2021 г.
Научно списание **http://www.mtc-aj.com** **статия № 2173**

ФИРМЕНАТА СИГУРНОСТТА КАТО КЛЮЧОВ ЕЛЕМЕНТ ЗА ЕФЕКТИВНО И ЕФИКАСНО УПРАВЛЕНИЕ

Дияна Гешкова Маринова
diana.marinova18@abv.bg

Висше транспортно училище „Тодор Каблешков”,
София, ул. „Гео Милев” № 158
РЕПУБЛИКА БЪЛГАРИЯ

Ключови думи: *фирмена сигурност, система, елементи, концепция за сигурност управление, конкурентоспособност.*

Резюме: *Докладът има за цел да разгледа, характеризира и определи теоретичните и практическите аспекти на фирмената сигурност, също така да определи и представи факторите, които влияят пряко върху сигурността. За целта са анализирани и изведени основните елементи при структурирането и изграждането на Концепция за сигурността на организацията, като са разгледани и представени основните външни и вътрешни заплахи за фирмената сигурност.*

„Тайната на ефективното управление е да знаеш онова, което другите не знаят, а добре изградената система за фирмена сигурност дава възможност на всеки мениджър/ ръководител да научи много за себе си, за екипа си, за околните.”

ВЪВЕДЕНИЕ

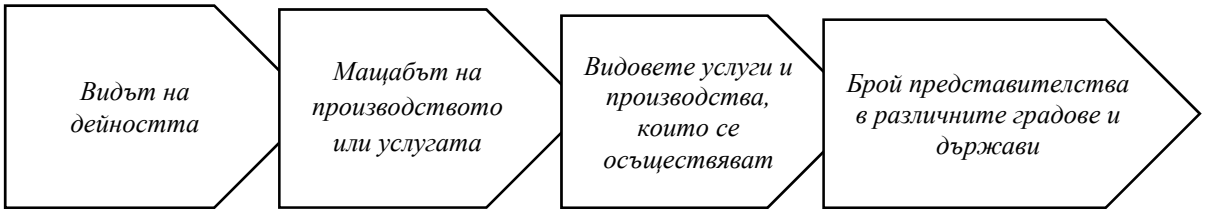
Голяма част от българските организации, независимо от техния характер – държавен или частен, които са решили да вземат мерки за сигурността си *„фирмената сигурност”* приключват с електронните системи за сигурност, живата охрана или договорът с фирма за охрана с технически средства. Организирайки тези две дейности много от мениджърите/ръководителите не си дават сметка, че това са само елементи на фирмената сигурност и обикновено са последната линия на защита, предназначена да сработи, когато са се провалили другите. Обикновено организациите решават проблемите със сигурността „на етапи”, както по отношение на отделните елементи, така и по отношение на отделни обекти и видове дейности. Масово се подценяват другите видове заплахи за организацията. От тук се установяват и повечето проблеми свързани със сигурността.

I. ТЕОРЕТИЧНИ АСПЕКТИ НА ФИРМЕНАТА СИГУРНОСТ

Фирмената сигурност е комплекс от взаимно свързани мероприятия, дейности и практики. Всичко трябва да е предварително структурирано и разработено като единна система – наречена **„Концепция за сигурност на организацията”.**

Фирмената сигурност може да се определи като съвкупност от специфични действия, практики и структура за физическа и информационна защита на хора, финансови средства, материална и интелектуална собственост, с цел осигуряване на устойчиво функциониране и създаване условия за постоянна, качествена и успешна работа.

За да се разработи ефективна система за фирмена сигурност, трябва да се анализира и да се отговори на въпросите за нейната потребност, необходимост и достатъчност. Естествено такава система зависи от много фактори.



Фигура 1. Фактори, които влияят върху фирмената сигурност
Източник: Собствени заключения

На първо място е видът дейност и услугите, които осъществява самата организация, но пряко влияние оказват и мащабът, наличието на различни по вид предлагани услуги, производства и дейности, наличието на офиси и производствени помещения в различни райони, градове и държави. Фактори от този род влияят и върху възможните заплахи и тяхната относимост.

Заплахите за управлението и дейността на една организация могат да се разделят на външни и вътрешни.

Към външните се отнасят заплахи от дейността, обкръжение, държавни политики, държавни органи, бюрокрация, корупция, трети лица, форсмажорни обстоятелства и много други.

Към вътрешните заплахи се отнасят действия от страна на съдружници, служители, недостатъци в управлението, недостатъци на техниката и технологиите и др.

Заплаха за сигурността на дадена организация може да представлява и промяната на политическата обстановка, промяната на демографските или социалните фактори, промяната на международните отношения, наличието на войни и конфликти в дадени райони влияят в по-голяма или по-малка степен на организацията, в зависимост от вида и нейната дейност и насоченост.

Социалните заплахи са свързани главно със стачки и епидемии. Политическите и международните заплахи са свързани с инфлация, промяна на приоритети, забрана на вид дейност, въвеждане на лицензионни режими, промяна на политическия строй, национализация и др.

Когато заплахите започнат да се реализират, в резултат на целенасочени действия срещу дадената организация, те се проявяват чрез различни видове атаки. Целта на атаките и последствията от тях в повечето случаи са:

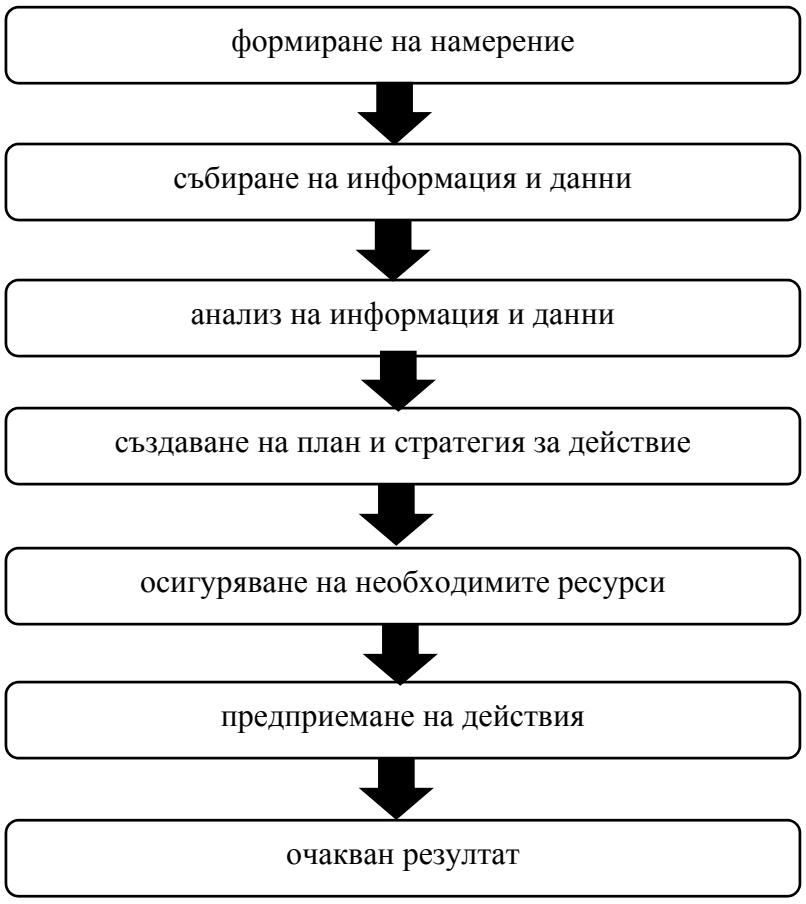
- ✓ *Финансови* – кражби, присвояване на средства, разхищения.
- ✓ *Информационни* – разпространение на фирмена тайна, компрометираща или зловредна информация, кражба на информация, унищожаване и повреждане на информация, документи и база данни.
- ✓ *Материални* – саботаж, повреди, унищожаване на имущество, кражби.
- ✓ *Вреда на дейността* – нарушение на нормалната дейност на организацията, забавяне или проваляне на процеси, преговори, изпълнение на договори и др.
- ✓ *Заплахи за здравето и живота на ръководители и персонал.*

Видовете атаки са изключително разнообразни. Например кражбата на информация от информационните системи най-често се свързва с хакерски атаки отвън, а се пренебрегват вътрешните фактори, като неправилно изградена система за информационна сигурност, умишлени или неволни действия на служители.

Подценява се социалното инженерство. Тотално се пренебрегва опасността от незаконно подслушване, което се прилага често, както от професионалисти, така и от аматьори и авантюристи, поради широкото разпространение и ниска себестойност на средствата за подслушване.

Във всяка атака участват хора. Външни и вътрешни. Няма голяма успешна атака, която да не е използвала информация или съучастие на вътрешен човек. Помощта от вътрешния човек бива доброволна или принудителна, умишлена или неумишлена, но във всички случаи демонстрира едно от най-важните и най уязвими звена на системата за сигурност – човешкият фактор. Човешките ресурси (персоналът) на всяка организация трябва да бъдат обект на особено внимание, както като потенциална заплаха, така и като най-уязвимо звено.

Всяка заплаха има предистория и причина. Обикновено всяка атака се реализира на няколко етапа (фигура 2):



Фигура 2. Етапи при реализиране на конкретна атака

Източник: Собствени заключения

- формиране на намерение, събиране на информация, анализ на информацията, изготвяне на план, осигуряване на необходимите ресурси, предприемане на действия, очакван резултат. По някога това става интуитивно и за секунди, а понякога е в

резултат на добре обмислен план и отнема месеци или години, но и двата случая има характерни признаци за всеки от етапите, които могат да бъдат доловени и анализирани с цел прилагане на превантивни или защитни мерки. Такива признаци и причини, обаче могат да бъдат доловени от професионалисти и при наличие на добре изградена система за фирмена сигурност.

Целта на фирмената сигурност е идентифициране и установяване на заплахи, изследване защитеността на обекти, създаване на система за защита на активите, предотвратяване и пресичане на инциденти и престъпления, разкриване на посегателства, охрана.

Системата за фирмена сигурност трябва да е изградена така, че да осигурява превенция. Това става чрез осигуряване на изпреварваща информация за външната среда, тоест чрез разузнавателна дейност; осигуряване на своевременна вътрешна информация – контра разузнавателна дейност, анализиране на получената информация и въз основа на това – определяне на нивата и основните направления на заплаха – анализ на риска.

Благодарение на тези дейности системата за фирмена сигурност може да позволява управление на риска. **Управлението на риска е основен вид дейност на системата за фирмена сигурност.** То позволява осъществяване на превенцията. Така се изпреварват събитията, а не да се предприемат действия след тях. Предотвратяването на престъпление или произшествие е много по-полезно и най-вече доходоносно за всяка организация, независимо от нейния характер – държавен или частен, отколкото неговото реално разкриване. Превантивната дейност създава стойност, а не изразходва средства за непланирани, малко ефективни и същевременно закъснели дейности и практики.

За да бъдат постигнати целите ѝ, системата за фирмена сигурност трябва да има възможност да противодейства на целия спектър от заплахи.

Изграждането само на алармена система и поставянето на охранител няма да реши въпроса с издаването на фирмена тайна, отклоняването на средства от мениджъри или съдружници, вредата от дейностите на корумпирани държавни чиновници или заплахата от поглъщане от други организации. От друга страна, добре изградената алармена система и добрата охрана могат да предотвратят атака от страна на криминален контингент или да откажат от враждебни действия нелоялни членове на персонала.

Елементите на системата за фирмена сигурност могат да се определят, като n – на брой, но всеки елемент трябва да е премерен, приложен и адаптиран на място, взаимно свързан с останалите и отговарящ адекватно на заплахите. Превишаване на вида и степента на прилаганите мерки за сигурност не повишава многократно нивото на сигурност, но със сигурност затруднява ежедневната дейност и изразходва финансови средства и човешки ресурс. Зле организираната система за сигурност, основана на непрофесионални действия и подценяване нивото на застрашеност е изключително опасна. Такава система дава фалшиво чувство за сигурност и успокоение.

Два са основните проблеми на фирмената сигурност във България. Първият е липсата на достатъчно професионалисти в областта. Това, че един човек е бил служител в полицията, службите, или армията не го прави специалист. Логистика на най-секретната служба, най-елитния ни разузнавач, охранителен полицай, или командир на мото стрелкова бригада, едва ли имат представа и за половината от елементите на фирмената сигурност. От другата страна са академичните среди в страната. Науката е водеща, но практическия опит е в основата на ежедневната дейност и успешните реализации. За да се избегне обучението на принципа „проба – грешка” е

необходимо да има стабилна теоретична основа, която да осигури прилагането на съвременните практически методи. Затова са необходими професионалисти, постоянно и непрекъснато продължаващо обучение, тъй като „*Обучението е равно на развитие, а без развитие, ние нямам как да бъдем конкурентноспособни и устойчиви при подобни ситуации", защото* казусите, свързани с фирмената сигурност са чести, разнородни и разнообразни и същевременно изискват адекватно реагиране за осигуряването и разрешаването им.

Вторият проблем е отношението на мениджърите/ръководителите. Те виждат как харчат пари за сигурност, а не виждат пряка възвращаемост. Не познават обстановката, заплахите и нивото на застрашеност, подценяват проблема или ситуацията. Ограничават по различни съображения сферата на дейност на звеното за сигурност.

Мениджърите са интелигентни хора, свикнали да вземат решения, и при добра основа и адекватно информационно осигуряване бързо ще се ориентират в проблемите на сигурността. Тяхната основна задача, обаче е да ръководят организацията, затова е необходимо да могат да разчитат на специалисти-професионалисти.

II. ПРАКТИЧЕСКИ АСПЕКТИ НА ФИРМЕНАТА СИГУРНОСТ НА ОРГАНИЗАЦИЯ В ДЪРЖАВНИЯ СЕКТОР

Създава се т. нар. „***техническо звено"***, което да ръководи и обезпечава ресурсно и технически дейностите, свързани с постигане на мрежова и информационна сигурност, в съответствие с нормативната уредба, политиките и целите за мрежова и информационна сигурност на конкретната организация. Утвърждават се вътрешни правила за мрежова и информационна сигурност, който да регламентират правилата за мрежова и информационна сигурност и да уреждат правата, задълженията и отговорностите на потребителите им. С тях се цели да се регламентира използването на информационните услуги и ресурси в съответствие със създадените процедури.

Техническото звено, чрез текущ и постоянен контрол следи, организирането и провеждането на вътрешните и външните одити, тестове за проникване и компрометиране на информационните системи на организацията, като изготвя доклади относно текущото състояние на мрежовата и информационна сигурност и дава препоръки за нейното подобряване.

Информационните активи може да включват хардуерни и софтуерни ресурси, данни. За информационните ресурси се създават и поддържат:

- инвентарни картони, определящи персоналната отговорност на всеки служител за зачислените му информационни ресурси(компютри, периферни устройства, софтуерни продукти и др.);
- данни за конкретен софтуерен продукт/информационна система на кои компютри и устройства се използват.

За категоризиране, контрол и управление на активите, техническото звено поддържа електронни бази данни с актуална информация за наличните информационни активи в организацията, както следва:

1. Регистър на комуникационното оборудване;
2. Регистър на периферната техника;
3. Регистър на компютърната техника;
4. Регистър на сървърните системи;
5. Регистър на софтуерните продукти;
6. Регистър на информационните системи;
7. Регистър за управление на промените;
8. Регистър на токъните.

При управлението и контрола на информационните активи трябва да се спазват следните правила:

Върху работните станции и сървърите в организацията се инсталират само софтуерни продукти, за които има придобито право за ползване (лиценз или програми, които не изискват лицензиране), като това се извършва само от определените за това специалисти от техническото звено или под техния надзор. Инсталирането и настройката на нов софтуер и хардуер се планира и всички лица, използващи засегнатите ресурси, се уведомяват предварително. Преди извършване на инсталация се правят резервни копия на софтуера, файловете и базите данни, в съответствие с разработен и утвърден от ръководителя на организацията план за непрекъснатост и план за възстановяване след срив.

Инсталирането, настройката и поддръжката на нов софтуер и хардуер се извършва в периоди с минимално натоварване на съответните ресурси.

Преди инсталиране в оперативно действащите системи на нов софтуер и хардуер, същите се проверяват в тестова среда максимално близка до реалната.

Рискът за сигурността е фактическо състояние, което може да доведе до повреждане или унищожаване на един или няколко информационни актива.

Оценката на риска се определя чрез изчисление на вероятността за повреждане или унищожаване въз основа на ефективността на съществуващите или планираните мерки за сигурност и влиянието, тежестта на възможните последици при настъпване на риска.

Рисковете за мрежова и информационна сигурност задължително се определят:

- ✓ по елементите на информационната сигурност (достъпност, цялостност, конфиденциалност), към които са насочени;
- ✓ по компонентите на информационната система (апаратура, софтуер, данни, поддържаща инфраструктура), към които са насочени;
- ✓ по начина на осъществяване (случайни/преднамерени действия, от природен/ технологичен характер и др.);
- ✓ по разположението на източника (вътре/извън информационната система).

Действията по управление на риска обхващат оценка на риска, изработване на ефективни и икономични мерки за въздействие на риска и оценка дали остатъчния риск е в приемливи граници. Управлението на риска се извършва чрез последователно прилагане на два типа циклично повтарящи се действия:

- оценка (преоценка) на риска;
- избор на ефективни и икономични средства за неговата неутрализация.

<u>При идентифициране на риск се предприема едно от следните действия:</u>

1. ликвидиране на риска (например чрез отстраняване на причиняващите го обстоятелства);

2. намаляване на риска (например чрез използване на допълнителни защитни средства);

3. приемане на риска и разработване на план за действия в обстановка на риск;

4. прехвърляне на риска (например чрез сключване на съответната застраховка, договор за поддръжка, аутсорсинг и др.).

<u>Процесът на управление на риска включва следните етапи:</u>

1. избор на анализируемите обекти и нивото на детайлизация на анализа;
2. избор на методология за оценка на риска;
3. идентификация на информационните активи;
4. анализ на заплахите, формулирани в международния стандарт ISO/IEC TR

13335:2000 и последствията от тях, откриване на уязвимите места в защитата;

5. оценка на рисковете;
6. избор на защитни мерки;
7. реализация и проверка на избраните мерки;
8. оценка на остатъчния риск - явява се начало на нов цикъл на оценка, който се провежда ако остатъчният риск не удовлетворява ръководството на ГДО. Оценка на остатъчния риск се извършва минимум веднъж в годината.

Видовете заплахи срещу мрежовата и информационната сигурност, формулирани в международния стандарт ISO/IEC TR 13335:2000, които могат да застрашат конфиденциалността, интегритета и достъпността, са следните:

- Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система.
- Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан код.
- Маскиране на потребителската идентичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея.
- Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност, ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения.
- Софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или за криптиране, или ако грешка в софтуера осигури възможност за нежелан достъп в информационна система.
- Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване.
- Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни данни и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно.
- Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни.
- Повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител.
- Не извършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни.
- Аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на авариите са увредени информационни системи или носители на данни.
- Технически аварии (например аварии в мрежите) могат да нарушат

интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа.

- Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност.
- Употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационната система, в която е настъпило такова събитие, и програмите и информацията се използват, за да се изменят съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код.
- Потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие.
- Липса на потвърждаване за получаване на данни може да застраши техния интегритет. Предпазните мерки за предотвратяване на не потвърждаването трябва да се прилагат в случаите, когато е важно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението.

За осигуряване на физическата защита на информационните системи ръководството на организацията трябва предприема следните мерки:

- ✓ мерки по управление на физическия достъп;
- ✓ противопожарни мерки;
- ✓ защита на поддържащата инфраструктура;
- ✓ защита на мобилните системи.

За постигане на информационна сигурност по отношение на човешките ресурси (персонала), трябва да се прилагат следните мерки за идентификацията на служителите и оправомощаването им да извършват определени действия по отношение на експлоатацията на информационните системи:

- ✓ достъпът на служителите до работните им станции и информационни системи се осъществява с уникални идентификатори (потребителско име и парола, токън и др.);
- ✓ служителите да имат право на достъп до информационни ресурси или до ресурси на други администрации, доколкото същите са им необходими за изпълнение на служебните задължения, съгласно длъжностната им характеристика или вътрешноведомствени актове (ако са упълномощени със заповед);

Всяка година служителите в организацията да преминават опреснителни курсове по фирмена сигурност, включващо обучение за конкретни действия при инциденти с мрежовата, информационна сигурност и т.н.

ЗАКЛЮЧЕНИЕ

В обобщение може да се подчертае, че *фирмената сигурност* е елемент от управлението на всяка успешна организация като цяло и тя се реализира от нейните структури за сигурност, в рамките на тяхната компетентност и в съответствие с възложените им задачи и предоставените им сили и средства за действие.

Потвърждава се фактът, че сигурност за една организация има тогава, когато основните ценности, нагласи, потребности и интереси на организацията не са подложени на никакви външни или вътрешни въздействия.

ЛИТЕРАТУРА:
[1] Василев, Е., „Фирмена сигурност“. Труд, 2000 С.
[2] Сандев, Г., „Сигурност на организациите“. Университетско издателство, Шумен, 2012.
[3] Стопански факултет, „Икономика и управление“, ЮЗУ „Неофит Рилски“, Благоевград, година V, бр. 4/2009 г.
[4] Павлов, Г., Пудин, К., „Информационна сигурност в организацията“, УИ „Стопанство“, 2011.
[5] Найденов, М., „Управление на фирмената сигурност“, Варна, 2002.

COMPANY SECURITY AS A KEY ELEMENT FOR EFFECTIVE AND EFFICIENT MANAGEMENT

Diyana Geshkova Marinova
diana.marinova18@abv.bg

Todor Kableshkov University of Transport
Sofia, 158 Geo Milev Str.158
THE REPUBLIC OF BULGARIA

Key words: *company security, system, elements, security management concept, competitiveness*

Abstract: *The report aims to consider, characterize and determine the theoretical and practical aspects of corporate security, as well as to identify and present the factors that directly affect security. For this purpose, the main elements in the structuring and construction of the Concept for the security of the organization are analyzed and presented, as the main external and internal threats to the company security are considered and presented.*